

COMPONENTI DI SICUREZZA: IL PANORAMA NORMATIVO





INTRODUZIONE

Il tema della sicurezza sui luoghi di lavoro è di assoluta importanza e gli enti normatori hanno sviluppato negli anni una serie di norme in continua evoluzione il cui punto focale resta la Direttiva Macchine.

Per assicurare la conformità della macchina, il costruttore deve verificare che soddisfi i requisiti di sicurezza elencati nella direttiva e garantire l'osservanza delle norme armonizzate pubblicate nella Gazzetta Ufficiale dell'Unione Europea relative al prodotto in questione.

Le norme di sicurezza per il macchinario sono di tre tipi:

- norme di tipo **A**, che fissano i principi generali validi per la progettazione di tutti i macchinari
- norme di tipo **B**, che trattano uno o più aspetti di sicurezza per un'ampia gamma di macchinari
- norme di tipo **C**, che trattano nel dettaglio una specifica categoria di macchine

Tra le norme di tipo **A** ricordiamo le EN ISO 12100 che riportano i concetti base ed i principi generali per la progettazione di macchinari sicuri e le EN ISO 14121 che descrivono un metodo per l'identificazione dei pericoli e la valutazione dei rischi.

Tra le norme di tipo **B** spiccano le EN ISO 13849 che forniscono gli strumenti per la progettazione delle parti di sistemi di comando legate alla sicurezza delle macchine ovvero dei sistemi di comando, costituiti da componenti realizzati con varie tecnologie, che servono a ridurre il rischio connesso all'utilizzo della macchina e le norme IEC 62061 che riguardano esclusivamente sistemi basati su tecnologie elettriche ed elettroniche. Una delle principali affinità tra la EN ISO 13849 e la IEC 62061 è che la prima definisce come parametro di sicurezza desiderato un indice chiamato PL (performance level) mentre la seconda identifica un parametro simile che viene denominato SIL (safety integrity level); entrambi rappresentano l'affidabilità della macchina in termini di probabilità di guasto pericoloso e possono essere messi in relazione tra di loro mediante la seguente tabella:

PL	SIL
a	Nessuna corrispondenza
b	1
c	1
d	2
e	3

Anche le norme EN982 e EN983 sono di tipo B e si occupano di sicurezza, ma a differenza delle precedenti sono relative ai componenti (rispettivamente idraulici e pneumatici) invece che alle parti di comando.

Quando, per la macchina in questione, esistono norme di tipo **C**, il costruttore può seguire direttamente tali norme per conseguire la presunzione di conformità alla Direttiva Macchine; se non esiste una norma di tipo C è comunque necessario seguire una strategia di riduzione del rischio come quella descritta nelle norme armonizzate di tipo A e B.

Dalla revisione denominata 98/37/EC la Direttiva Macchine non tratta solamente le macchine ma anche i componenti di sicurezza, ovvero quei componenti appositamente prodotti e commercializzati allo scopo di realizzare una funzione di sicurezza e la cui rottura o malfunzionamento mette a repentaglio la sicurezza e la salute delle persone.

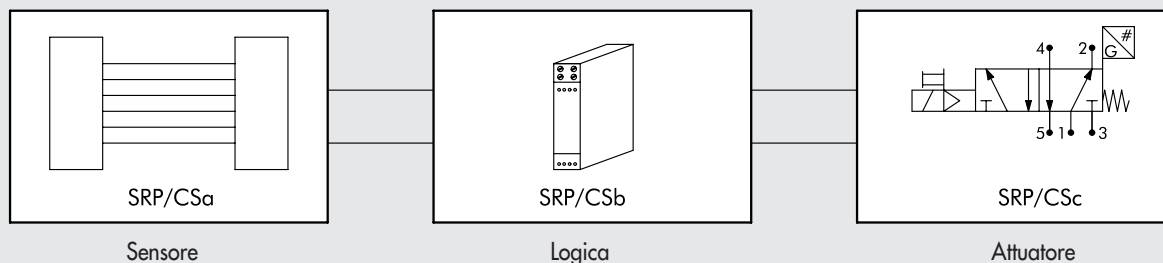
LA NORMA EN ISO 13849

Quando non esistono norme specifiche di tipo C per la macchina in questione, il costruttore può utilizzare la strategia di riduzione del rischio indicata nella EN ISO 13849.

La norma è divisa in due parti: nella prima parte vengono riportati i principi generali ed il metodo da seguire; la seconda parte è dedicata alla validazione dei risultati.

Secondo quanto riportato nella prima parte della norma, il progettista della macchina può ridurre il rischio progettando opportune parti del comando legate alla sicurezza (SRP/CS - safety-related parts of a control system) che svolgono una o più funzioni di sicurezza, quali l'arresto d'emergenza, la prevenzione dall'avviamento inatteso, l'isolamento e la dissipazione dell'energia, ecc...

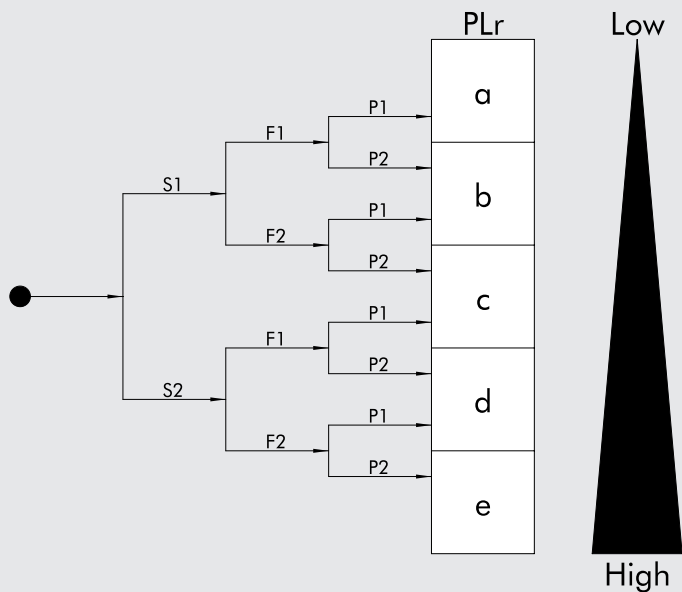
Riportiamo ad esempio una funzione costituita da tre SRP/CS: una barriera di sicurezza (ingresso - sensore), un PLC (elaborazione - logica) e una valvola (uscita - attuatore); in caso di intrusione la barriera invia un segnale al PLC che comanda la valvola la quale a sua volta ha il compito di mettere a scarico una sezione del circuito pneumatico in pressione eseguendo in tal modo la funzione di isolamento e dissipazione dell'energia pneumatica.



Per ogni funzione di sicurezza si deve determinare il Performance Level richiesto (PLr) secondo la procedura indicata nell'allegato A della norma.

A tale scopo vanno valutati:

- la gravità della lesione (S) derivante dall'eventuale guasto
- la frequenza di esposizione al pericolo (F)
- la possibilità di evitare il pericolo (P)



Se ad esempio la gravità della lesione derivante dal guasto è bassa e/o la frequenza di esposizione al pericolo è bassa e/o la possibilità di evitare il pericolo è elevata, il PLr sarà basso. Viceversa se la gravità e/o la frequenza di esposizione sono alte e/o la possibilità di evitare il pericolo è bassa allora il PLr per quella funzione di sicurezza sarà elevato.

Quindi il progettista della macchina per ogni SRP/CS o combinazione di SRP/CS che svolgono una funzione di sicurezza deve determinare il livello di prestazione PL ottenibile.

A tale calcolo devono essere utilizzati alcuni dati, tra i quali riportiamo:

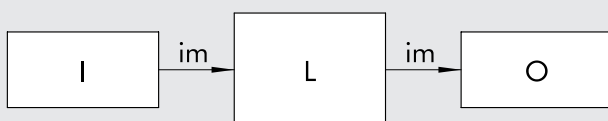
- MTTFd (Mean Time To Failure) dei singoli componenti
- DC (Diagnostic Coverage)
- CCF (Common Cause Failure)
- Struttura della funzione
- La conformità dei componenti utilizzati ai principi di sicurezza di base e/o ben provati

L'**MTTFd**, che è il tempo medio tra due guasti pericolosi, si può ottenere avendo a disposizione i dati sul ciclo di lavoro della funzione di sicurezza ed il B10d dei componenti, ovvero il numero di cicli ai quali il 10% dei componenti in questione si guasta in maniera pericolosa; il B10d è pari al doppio del B10 che a sua volta è un indice di affidabilità del componente ricavabile seguendo quanto indicato nelle norme EN ISO 19973.

I valori del B10d dei prodotti Metal Work sono pubblicati sul sito web: http://www.metalwork.it/ita/dirett_macchine.html.

DC e **CCF**, ovvero copertura diagnostica e stima dei guasti di causa comune, vengono ricavati con l'ausilio delle appendici alla norma EN ISO 13849-1; per la determinazione del DC ci si può aiutare con strumenti per l'analisi delle modalità e degli effetti dei guasti come, per esempio, la FMEA.

La **struttura della funzione** dipende dalla sua architettura. Si può avere ad esempio un'architettura a singolo canale non monitorato:



Dove:

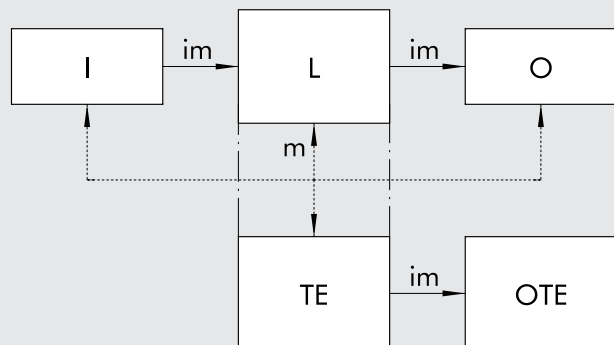
im: mezzo di interconnessione

I: dispositivo di ingresso, per esempio sensore

L: logica

O: dispositivo di uscita, per esempio valvola

Si passa quindi all'architettura semplice canale con diagnostica; in questo caso esiste un modulo denominato Test Equipment (TE) che fornisce un output (OTE) legato in qualche modo allo stato della funzione di sicurezza:



Dove:

im: mezzo di interconnessione

I: dispositivo di ingresso, per esempio sensore

L: logica

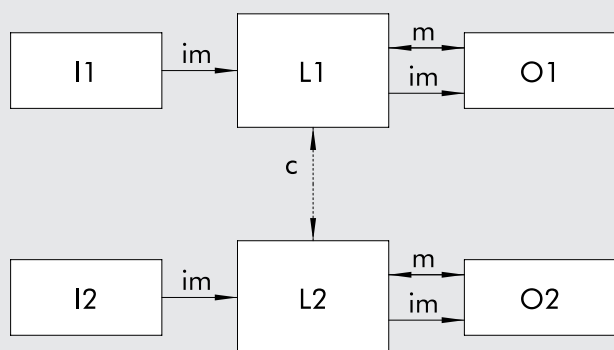
m: mezzo di sorveglianza

O: dispositivo di uscita, per esempio valvola

OTE: OUTPUT del Test Equipment

TE: Test Equipment

Un terzo esempio è un'architettura a doppio canale che sfrutta la ridondanza della funzione: se una linea si guasta, l'altra rimane attiva:



Dove:

im: mezzo di interconnessione

I1, I2: dispositivo di ingresso, per esempio sensore

L1, L2: logica

m: mezzo di sorveglianza

O1, O2: dispositivo di uscita, per esempio valvola

c: sorveglianza incrociata

Per la **conformità dei componenti utilizzati ai principi di sicurezza di base e/o ben provati** si tratta di valutare una serie di considerazioni riportate nelle norme EN ISO 13849 che garantiscono che le SRP/CS ed i relativi componenti rispondano a taluni principi di progettazione, costruzione ed assemblaggio.

Con tali dati il progettista della macchina può determinare la categoria della funzione di sicurezza (che può essere, in ordine crescente di importanza, B, 1, 2, 3 oppure 4) ed il PL raggiunto; si tratta quindi verificare che sia maggiore o uguale al PLr richiesto.